GENERIC PARABOLIC POINTS ARE ISOLATED IN POSITIVE CHARACTERISTIC

KARL-OLOF LINDAHL[†] AND JUAN RIVERA-LETELIER[‡]

Abstract. We study analytic germs in one variable having a parabolic fixed point at the origin, over an ultrametric ground field of positive characteristic. It is conjectured that for such a germ the origin is isolated as a periodic point. Our main result is an affirmative solution of this conjecture in the case of a generic germ with a prescribed multiplier. The genericity condition is explicit: That the power series is minimally ramified, *i.e.*, that the degree of the first non-linear term of each of its iterates is as small as possible. Our main technical result is a computation of the first significant terms of a minimally ramified power series. From this we obtain a lower bound for the norm of nonzero periodic points, from which we deduce our main result. As a by-product we give a new and self-contained proof of a characterization of minimally ramified power series in terms of the iterative residue.

1. Introduction

In this article, we are interested in the dynamics near a parabolic cycle of analytic maps in positive characteristic. Recall that a periodic point ζ_0 of minimal period n of an analytic map f in one variable is *rationally indifferent* or *parabolic* if $(f^n)'(\zeta_0)$ is a root of unity, and it is *irrationally indifferent* if $(f^n)'(\zeta_0)$ is not a root of unity, but $|(f^n)'(\zeta_0)| = 1$.

In the complex setting, Yoccoz showed that for an irrationally indifferent cycle of a quadratic map there is the following dichotomy: Either the map is locally linearizable near the cycle and then each point in this cycle is isolated as a periodic point, or every neighborhood of the cycle contains a cycle of strictly larger minimal period, see [Yoc95]. In contrast, for an ultrametric ground field of characteristic zero only the first alternative occurs: Every irrationally indifferent cycle is locally linearizable [HY83], and hence every point in the cycle is isolated as a periodic point. The case of an ultrametric field of positive characteristic is more subtle, since irrationally indifferent cycles are usually not locally linearizable, see for example [Lin04, Theorem 2.3] or [Lin10, Theorem 1.1]. Nevertheless, every irrationally indifferent periodic point is isolated as a periodic point [LRL16, Corollary 1.1].

[†] This research was supported by the by the Royal Swedish Academy of Sciences and the Swedish Research and Education in Mathematics Foundation SVeFUM.

[‡] This research was partially supported by FONDECYT grant 1141091, Chile.

In this paper we focus on parabolic cycles. An analytic map is never locally linearizable near a parabolic cycle, except in the trivial case where an iterate of the map is the identity near the cycle. Thus, the question that remains is whether (non-trivial) parabolic periodic points are isolated. For an ultrametric ground field of characteristic zero the answer is affirmative: The positive residue characteristic case follows from the fact that periodic points are the zeros of the iterative logarithm, see [RL03, Proposition 3.6] and also [Lub94] for the case where the ground field is discretely valued; The zero residue characteristic case follows from elementary facts, see for example [LRL16, Lemma 2.1].

Thus, it only remains the case of parabolic cycles in positive characteristic. In [LRL16] we proposed the following conjecture.

Conjecture 1.1 ([LRL16], Conjecture 1.2)**.** *In positive characteristic, every parabolic periodic point is either isolated as a periodic point, or has a neighborhood on which an iterate of the map is the identity.*

Our main result is a solution of this conjecture for generic parabolic periodic points.

Main Theorem. *In positive characteristic, every generic parabolic periodic point is isolated as a periodic point.*

The proof of the Main Theorem relies on the connection between the geometric location of periodic points of power series with integer coefficients, and the lower ramification numbers of wildly ramified field automorphisms that was established in [LRL16]. Lower ramification numbers of wildly ramified field automorphisms have previously been studied by Sen [Sen69], Keating [Kea92], Laubie and Saïne [LS98], Wintenberger [Win04], among others.

We now proceed to describe the content and proof of the Main Theorem in more precise terms. Replacing the map by an iterate if necessary, we restrict to the case of fixed points. Moreover, after conjugating by a translation we assume the fixed point is the origin. So, from now on we restrict to study power series $f(\zeta)$ such that $f(0) = 0$ and such that $f'(0)$ is a root of unity. We call such a power series *parabolic.* Finally, after a scale change we can restrict to the case of power series with integer coefficients. In the case where the ground field is algebraically closed, this last condition is equivalent to the condition that the power series is convergent and univalent on the open unit disk, see for example [RL03, §1.3]. So these normalizations are analogous to those used in the complex setting by Yoccoz in [Yoc95].

The genericity condition in the Main Theorem is described explicitly in terms of the lower ramification numbers of the map: It requires that the lower ramification numbers are as small as possible. Such power series are called *minimally ramified*, see §1.1 for precisions. So the Main Theorem is a direct consequence of 2 independent facts:

A. Minimally ramified parabolic power series are generic (Theorem A in §1.1);

B. For a parabolic power series that is minimally ramified, the origin is isolated as a periodic point (Corollary C in §1.2).

Minimally ramified power series appear naturally when studying "optimal cycles" of irrationally indifferent periodic points, see [LRL16]. They were first introduced in a more restricted setting by Laubie, Movahhedi, and Salinier in [LMS02], in connection with Lubin's conjecture in [Lub94].

Our main technical result is a calculation of the first significant terms of the iterates of power series in a certain normal form (Main Lemma in §3). This allows us to give a new and self-contained proof of the characterization of minimally ramified power series given in [LRL16] (Theorem D in §1.3).

We proceed to describe our main results in more detail. Throughout the rest of the introduction we fix a prime number p and a field k of characteristic p.

1.1. **Minimally ramified power series are generic.** Denote by $\operatorname{ord}(\cdot)$ the valuation on $k[[\zeta]]$ defined for a nonzero power series as the lowest degree of its nonzero terms, and for the zero power series 0 by $\operatorname{ord}(0) = +\infty$.

Definition 1.2. For a power series $g(\zeta)$ in $k[[\zeta]]$ satisfying $g(0) = 0$ and $g'(0) = 1$, define for each integer $n \geq 0$

$$i_n(g) := \operatorname{ord}\left(\frac{g^{p^n}(z) - z}{z}\right).$$

If $g(\zeta)$ is as in the definition and $n \geq 1$ is such that $i_n(g)$ is finite, then $i_0(g)$, …, $i_{n-1}(g)$ are all finite and we have

$$i_0(g) < i_1(g) < \cdots < i_n(g),$$

see for example [LRL16, Lemma 3.6].

Let $f(\zeta)$ be a parabolic power series in $k[[\zeta]]$ and denote by q the order of $f'(0)$, so that $f^q(0) = 0$ and $(f^q)'(0) = 1$. Then for every integer $n \geq 0$ we have

$$i_n(f^q) \geq q\frac{p^{n+1} - 1}{p - 1}, \tag{1.1}$$

see [LRL16, Proposition 3.2]. This motivates the following definition.

Definition 1.3. Let $f(\zeta)$ be a parabolic power series in $k[[\zeta]]$ and denote by q the order of $f'(0)$. Then f is *minimally ramified* if equality holds in (1.1) for every $n \geq 0$.

Roughly speaking, the following result asserts that among parabolic power series with a prescribed multiplier, those that are minimally ramified are generic.

Theorem A. *Let p be a prime number, k a field of characteristic p, and F the prime field of k. Fix a root of unity γ in k and denote by q its order.*

Then there is a nonzero polynomial $M_q(x_1, \ldots, x_{2q})$ with coefficients in $F(\gamma)$, such that a power series $f(\zeta)$ in $k[[\zeta]]$ of the form

$$f(\zeta) = \gamma\zeta \left(1 + \sum_{i=1}^{+\infty} c_i \zeta^i\right) \tag{1.2}$$

is minimally ramified if and only if $M_q(c_1, \ldots, c_{2q}) \neq 0$.

1.2. **Periodic points of minimally ramified parabolic power series.** Now we turn to periodic points of parabolic power series that are minimally ramified. For such a power series that has integer coefficients, we estimate from below the norm of nonzero periodic points. The estimate is in terms of some invariants that we proceed to describe.

In this section we fix a parabolic power series $f(\zeta)$ in $k[[\zeta]]$ and denote by q the order of $\gamma := f'(0)$. We assume $i_0(f^q) = q$, which is weaker than f being minimally ramified.

The first invariant is the coefficient $\delta_0(f^q)$ of ζ^{q+1} in f^q so that $\delta_0(f^q) \neq 0$ and that

$$f^q(\zeta) = \zeta\left(1 + \delta_0(f^q)\zeta^q + \cdots\right).$$

The coefficient $\delta_0(f^q)$ is invariant under conjugacy by power series that are tangent to the identity at $\zeta = 0$ (Lemma 2.2).

The second invariant is the "iterative residue" introduced in [LRL16, §4]. It is a positive characteristic analog of the invariant introduced in the complex setting by Écalle in [Éca75]. To define it, suppose first $\gamma = 1$, and let a_1 and a_2 in k be such that $f(\zeta)$ is of the form

$$f(\zeta) = \zeta\left(1 + a_1\zeta + a_2\zeta^2 + \cdots\right).$$

Our hypothesis $i_0(f) = 1$ implies $a_1 \neq 0$. The *iterative residue* $\text{résit}(f)$ of f is defined by

$$\text{résit}(f) := 1 - \frac{a_2}{a_1^2}.$$

Suppose now that $\gamma \neq 1$, so $q \geq 2$. Then f is conjugated to a power series of the form

$$g(\zeta) = \gamma\zeta\left(1 + \sum_{j=1}^{+\infty} a_j \zeta^{jq}\right), \tag{1.3}$$

see Lemma 3.3 or [LRL16, Proposition 4.1]. Our hypothesis $i_0(f^q) = q$ implies $a_1 \neq 0$ (Lemma 2.2 and Corollary 3.1 or [LRL16, Proposition 4.1]). The *iterative residue* $\text{résit}(f)$ of f is defined by

$$\text{résit}(f) := \frac{q+1}{2} - \frac{a_2}{a_1^2};^{*}$$

It only depends on f and not on g. In all the cases $\text{résit}(f)$ is a conjugacy invariant of f, see [LRL16, Lemma 4.3].

*Note that in the case $p = 2$ the integer q is odd, so $\frac{q+1}{2}$ defines an element of k.

Suppose k is endowed with a norm $|\cdot|$ and denote by $\mathcal{O}_k$ the ring of integers of $(k, |\cdot|)$ and by $\mathfrak{m}_k$ its maximal ideal. Then the minimal period of each periodic point of f in $\mathfrak{m}_k \setminus \{0\}$ is of the form qp^n, for some integer $n \geq 0$, see for example [LRL16, Lemma 2.1].

Theorem B. *Let p be a prime number and $(k, |\cdot|)$ an ultrametric field of characteristic p. Let $f(\zeta)$ be a parabolic power series in $\mathcal{O}_k[[\zeta]]$ and denote by q the order of $f'(0)$. Then for every integer $n \geq 1$ and every periodic point ζ_0 of f of minimal period qp^n, we have*

$$|\zeta_0| \geq \begin{cases} |\delta_0(f^q)|^{\frac{1}{q}} \cdot |\text{résit}(f)|^{\frac{1}{qp}} & \text{if } p \text{ is odd} \\ & \text{or if } p = 2 \text{ and } n = 1; \\ |\delta_0(f^q)|^{\frac{1}{q}} \cdot |\text{résit}(f)\,(1 - \text{résit}(f))|^{\frac{1}{4q}} & \text{if } p = 2 \text{ and } n \geq 2. \end{cases}$$

In the case f is minimally ramified, we have $\text{résit}(f) \neq 0$, and also $\text{résit}(f) \neq 1$ if $p = 2$, see [LRL16, Theorem E] or Theorem D in §1.3. So the following corollary is a direct consequence of the previous theorem and of [LRL16, Lemma 2.1].

Corollary C. *Let $(k, |\cdot|)$ be an ultrametric field of positive characteristic. Then for each parabolic power series in $\mathcal{O}_k[[\zeta]]$ that is minimally ramified, the origin is isolated as a periodic point.*

1.3. **Strategy and organization.** Our main technical result is a calculation of the first significant terms of the iterates of a power series in $k[[\zeta]]$ of the form (1.3). This is stated as the Main Lemma in §3. A direct consequence is an explicit condition on the coefficients a_1 and a_2 for the power series $g(\zeta)$ to be minimally ramified (Corollary 3.1). Theorem A is obtained from this result using that every parabolic power series is conjugated to a power series of the form (1.3) by an invertible map in $\mathcal{O}_k[[\zeta]]$ (Lemma 3.3). The same strategy allows us to give a new and self-contained proof of the following characterization of minimally ramified power series,[†] see §3.1.

Theorem D ([LRL16], Theorem E)**.** *Let p be a prime number and k a field of characteristic p. Moreover, let $f(\zeta)$ be a parabolic power series in $k[[\zeta]]$, and denote by q the order of $f'(0)$. If p is odd (resp. $p = 2$), then f is minimally ramified if and only if*

$$i_0(f^q) = q \textit{ and } \text{résit}(f) \neq 0$$

$$(\textit{resp. } i_0(f^q) = q, \text{résit}(f) \neq 0, \textit{ and } \text{résit}(f) \neq 1)\,.$$

To prove Theorem B, we first prove a version for parabolic power series of the Period Points Lower Bound of [LRL16] (Lemma 2.4). Combined with the Main Lemma in §3 this yields a lower bound for the norm of the periodic points of a power series of the form (1.3) (Corollary 3.2). Theorem B is then

[†] The proof of this result in [LRL16] relies on [LS98, Corollary 1]; the Main Lemma allows us to give a direct proof that avoids this last result.

obtained using again that every parabolic power series is conjugated to a power series of the form (1.3) by an invertible map in $\mathcal{O}_k[[\zeta]]$ (Lemma 3.3).

After some preliminaries in §2, we state the Main Lemma and deduce its Corollaries 3.1 and 3.2 in the first part of §3. The proofs of Theorems A, B, and D assuming the Main Lemma are given in §3.1. Finally, the proof of the Main Lemma is given in §4. As mentioned above, the Main Theorem is a direct consequence of Theorems A and B.

1.4. **Acknowledgement.** We would like to thank the referee for comments and corrections that helped us improve the presentation.

2. Periodic points of parabolic power series

After some preliminaries in §2.1, in §2.2 we give some basic facts about periodic points of parabolic power series with integer coefficients. In particular, we give a general lower bound for the distance to the origin of a periodic point (Lemma 2.4) that is used in the proof Theorem B.

2.1. **Preliminaries.** Given a ring R and an element a of R, we denote by $\langle a \rangle$ the ideal of R generated by a.

Let $(k, |\cdot|)$ be an ultrametric field. Denote by $\mathcal{O}_k$ the ring of integers of k, by $\mathfrak{m}_k$ the maximal ideal of $\mathcal{O}_k$, and by $\widetilde{k} := \mathcal{O}_k/\mathfrak{m}_k$ the residue field of k. Moreover, denote the projection in $\widetilde{k}$ of an element a of $\mathcal{O}_k$ by $\widetilde{a}$; it is the *reduction of a*. The *reduction* of a power series $f(\zeta)$ in $\mathcal{O}_k[[\zeta]]$ is the power series $\widetilde{f}(z)$ in $\widetilde{k}[[z]]$ whose coefficients are the reductions of the corresponding coefficients of f.

For a power series $f(\zeta)$ in $\mathcal{O}_k[[\zeta]]$, the *Weierstrass degree* $\mathrm{wideg}(f)$ *of f* is the order in $\widetilde{k}[[z]]$ of the reduction $\widetilde{f}(z)$ of $f(\zeta)$. When $\mathrm{wideg}(f)$ is finite, the number of zeros of f in $\mathfrak{m}_k$, counted with multiplicity, is less than or equal to $\mathrm{wideg}(f)$; see for example [Lan02, §VI, Theorem 9.2].

A power series $f(\zeta)$ in $\mathcal{O}_k[[\zeta]]$ converges in $\mathfrak{m}_k$. If in addition $|f(0)| < 1$, then by the ultrametric inequality f maps $\mathfrak{m}_k$ to itself. In this case a point ζ_0 in $\mathfrak{m}_k$ is *periodic for f*, if there is an integer $n \geq 1$ such that $f^n(\zeta_0) = \zeta_0$. In this case ζ_0 *is of period n*, and n is a *period of* ζ_0. If in addition n is the least integer with this property, then n is the *minimal period of* ζ_0 and $(f^n)'(\zeta_0)$ is the *multiplier of* ζ_0. Note that an integer $n \geq 1$ is a period of ζ_0 if and only if it is divisible by the minimal period of ζ_0.

The following definition is consistent with the definition of $\delta_0(\cdot)$ in the introduction.

Definition 2.1. Let p be a prime number and k field of characteristic p. For a power series $g(\zeta)$ in $k[[\zeta]]$ satisfying $g(0) = 0$ and $g'(0) = 1$, define for each integer $n \geq 0$ the element $\delta_n(g)$ of k as follows: Put $\delta_n(g) := 0$ if $i_n(g) = +\infty$, and otherwise let $\delta_n(g)$ be the coefficient of $\zeta^{i_n(g)+1}$ in the power series $g^{p^n}(\zeta) - \zeta$.

Note that in the case where $i_n(g)$ is finite, $\delta_n(g)$ is nonzero. Moreover, if k is an ultrametric field and $g(\zeta)$ is in $\mathcal{O}_k[[\zeta]]$, then $g^{p^n}(\zeta) - \zeta$ is also in $\mathcal{O}_k[[\zeta]]$, and therefore $\delta_n(g)$ is in $\mathcal{O}_k$.

Lemma 2.2. *Let p be a prime number and k field of characteristic p. Moreover, let $f(\zeta)$ and $\widehat{f}(\zeta)$ be parabolic power series in $k[[\zeta]]$ and denote by q the order of $f'(0)$. Suppose there is a power series $h(\zeta)$ in $k[[\zeta]]$ such that*

$$h(0) = 0, h'(0) \neq 0, \text{ and } f \circ h = h \circ \widehat{f}.$$

Then $\widehat{f}'(0) = f'(0)$ and for every integer $n \geq 0$ we have

$$i_n(\widehat{f}^q) = i_n(f^q) \text{ and } \delta_n(\widehat{f}^q) = (h'(0))^{i_n(f^q)} \cdot \delta_n(f^q).$$

Proof. From $f \circ h = h \circ \widehat{f}$ we have $f'(0)h'(0) = h'(0)\widehat{f}'(0)$. Together with our assumption $h'(0) \neq 0$ this implies $\widehat{f}'(0) = f'(0)$.

Fix an integer $n \geq 0$, and note that $f^{qp^n} \circ h = h \circ \widehat{f}^{qp^n}$. If $i_n(f) = +\infty$, then $\delta_n(f^{qp^n}) = 0$ and $f^{qp^n}(\zeta) = \zeta$. This implies $\widehat{f}^{qp^n}(\zeta) = \zeta$, so $i_n(\widehat{f}^q) = +\infty$ and $\delta_n(\widehat{f}^q) = 0$. This proves the lemma when $i_n(f) = +\infty$. Interchanging the roles of f and $\widehat{f}$, this also proves the lemma when $i_n(\widehat{f}) = +\infty$. Suppose $i_n(f)$ and $i_n(\widehat{f})$ are finite, and put

$$i_n := i_n(f^q), \; \widehat{i}_n := i_n(\widehat{f}^q), \text{ and } h(\zeta) = \zeta \cdot \sum_{i=0}^{+\infty} c_i \zeta^i.$$

Then we have

$$\begin{aligned} f^{qp^n} \circ h(\zeta) &\equiv \zeta \left(c_0 + c_1\zeta + \cdots + c_{i_n}\zeta^{i_n}\right)\left(1 + \delta_n(f^q)(c_0\zeta)^{i_n}\right) \mod \left\langle \zeta^{i_n+2} \right\rangle \\ &\equiv \zeta \left(c_0 + c_1\zeta + \cdots + c_{i_n-1}\zeta^{i_n-1} + \left(c_{i_n} + c_0^{i_n+1}\delta_n(f^q)\right)\zeta^{i_n}\right) \\ &\qquad \mod \left\langle \zeta^{i_n+2} \right\rangle. \end{aligned}$$

On the other hand,

$$\begin{aligned} h \circ \widehat{f}^q(\zeta) &\equiv \zeta \left(1 + \delta_n(\widehat{f}^q)\zeta^{\widehat{i}_n}\right)\left(c_0 + c_1\zeta + \cdots + c_{\widehat{i}_n}\zeta^{\widehat{i}_n}\right) \mod \left\langle \zeta^{\widehat{i}_n+2} \right\rangle. \\ &\equiv \zeta \left(c_0 + c_1\zeta + \cdots + c_{\widehat{i}_n-1}\zeta^{\widehat{i}_n-1} + \left(c_{\widehat{i}_n} + c_0\delta_n(\widehat{f}^q)\right)\zeta^{\widehat{i}_n}\right) \\ &\qquad \mod \left\langle \zeta^{\widehat{i}_n+2} \right\rangle. \end{aligned}$$

Comparing coefficients and using that c_0, $\delta_n(f^q)$, and $\delta_n(\widehat{f}^q)$ are all different from zero, we conclude that $i_n = \widehat{i}_n$ and that $\delta_n(\widehat{f}^q) = c_0^{i_n}\delta_n(f^q)$, as wanted. □

2.2. **Periodic points of parabolic power series.** The following lemma is well-known, see for example [LRL16, Lemma 2.1] for a proof.

Lemma 2.3. *Let p be a prime number and k an ultrametric field of characteristic p. Moreover, let $f(\zeta)$ be a parabolic power series in $k[[\zeta]]$ and denote* *by q the order of $f'(0)$. Then q is not divisible by p, and the minimal period of each periodic point of f is of the form qp^n for some integer $n \geq 0$.*

The following lemma is a version of [LRL16, Lemma 2.3] for parabolic power series, with a similar proof. We have restricted to ground fields of positive characteristic for simplicity. It is one of the ingredients in the proof of Theorem B. Before stating the lemma we recall that for a power series $f(\zeta)$ in $\mathcal{O}_k[[\zeta]]$, the Weierstrass degree $\operatorname{wideg}(f)$ of f is the order in $\widetilde{k}[[z]]$ of the reduction $\widetilde{f}(z)$ of $f(\zeta)$.

Lemma 2.4 (Periodic points lower bound for parabolic series)**.** *Let p be a prime number and $(k, |\cdot|)$ an ultrametric field of characteristic p. Moreover, let $f(\zeta)$ be a parabolic power series in $\mathcal{O}_k[[\zeta]]$ and denote by q the order of $f'(0)$. Then the following properties hold.*

1. *Let w_0 in $\mathfrak{m}_k$ be a periodic point of f of minimal period q. In the case $q = 1$, assume $w_0 \neq 0$. Then we have*
$$|w_0| \geq |\delta_0(f^q)|^{\frac{1}{q}}, \tag{2.1}$$
with equality if and only if
$$\operatorname{wideg}\left(f^q(\zeta) - \zeta\right) = i_0(f^q) + q + 1. \tag{2.2}$$
Moreover, if (2.2) holds, then the cycle containing w_0 is the only cycle of minimal period q of f in $\mathfrak{m}_k \setminus \{0\}$, and for every point w_0' in this cycle $|w_0'| = |\delta_0(f^q)|^{\frac{1}{q}}$.
2. *Let $n \geq 1$ be an integer and ζ_0 in $\mathfrak{m}_k$ a periodic point of f of minimal period qp^n. If in addition $i_n(f^q) < +\infty$, then we have*
$$|\zeta_0| \geq \left|\frac{\delta_n(f^q)}{\delta_{n-1}(f^q)}\right|^{\frac{1}{qp^n}}, \tag{2.3}$$
with equality if and only if
$$\operatorname{wideg}\left(\frac{f^{qp^n}(\zeta) - \zeta}{f^{qp^{n-1}}(\zeta) - \zeta}\right) = i_n(f^q) - i_{n-1}(f^q) + qp^n. \tag{2.4}$$
Moreover, if (2.4) holds, then the cycle containing ζ_0 is the only cycle of minimal period qp^n of f in $\mathfrak{m}_k$, and for every point ζ_0' in this cycle $|\zeta_0'| = \left|\frac{\delta_n(f^q)}{\delta_{n-1}(f^q)}\right|^{\frac{1}{qp^n}}$.

The proof of this lemma is below, after the following lemmas.

Lemma 2.5. [LRL16, Lemma 2.2] *Let $(k, |\cdot|)$ be a complete ultrametric field and $g(\zeta)$ a power series in $\mathcal{O}_k[[\zeta]]$ such that $|g(0)| < 1$. Then for each integer $m \geq 1$ the power series $g(\zeta) - \zeta$ divides $g^m(\zeta) - \zeta$ in $\mathcal{O}_k[[\zeta]]$.*

Lemma 2.6. *Let k be a complete ultrametric field and let $h(\zeta)$ be a power series in $\mathcal{O}_k[[\zeta]]$. If ξ is a zero of h in $\mathfrak{m}_k$, then $\zeta - \xi$ divides $h(\zeta)$ in $\mathcal{O}_k[[\zeta]]$.*

Proof. Put $T(\zeta) = \zeta + \xi$ and note that $h \circ T(\zeta)$ vanishes at $\zeta = 0$ and is in $\mathcal{O}_k[[\zeta]]$. This implies that ζ divides $h \circ T(\zeta)$ in $\mathcal{O}_k[[\zeta]]$. Letting $g(\zeta) := h \circ T(\zeta)/\zeta$, it follows that the power series $g \circ T^{-1}(\zeta) = h(\zeta)/(\zeta - \xi)$ is in $\mathcal{O}_k[[\zeta]]$, as wanted. □

Proof of Lemma 2.4. Replacing k by one of its completions if necessary, assume k complete.

We use the fact that, since $|f'(0)| = 1$, the power series f maps $\mathfrak{m}_k$ to itself isometrically, see for example [RL03, §1.3]. We also use several times that when $\mathrm{wideg}(f)$ is finite, we have:

I. The Weierstrass degree $\mathrm{wideg}(f)$ of f equals the degree of the lowest degree term of f whose coefficient is of norm equal to 1;

II. The number of zeros of f in $\mathfrak{m}_k$, counted with multiplicity, is less than or equal to $\mathrm{wideg}(f)$.

1. To prove (2.1), let w_0 in $\mathfrak{m}_k$ be a periodic point of f of minimal period q. Note that every point in the forward orbit O of w_0 under f is a zero of the power series $(f^q(\zeta) - \zeta)/\zeta$, and that the coefficient of the lowest degree term of this power series is $\delta_0(f^q)$. On the other hand, O consists of q points, and, since f maps $\mathfrak{m}_k$ to itself isometrically, all the points in O have the same norm. Applying Lemma 2.6 inductively with ξ replaced by each element of O, it follows that $\prod_{w_0' \in O}(\zeta - w_0')$ divides $f^q(\zeta) - \zeta$ in $\mathcal{O}_k[[\zeta]]$. That is, the power series

$$\frac{f^q(\zeta) - \zeta}{\zeta} \Big/ \prod_{w_0' \in O} (\zeta - w_0') \tag{2.5}$$

is in $\mathcal{O}_k[[\zeta]]$. Note that the lowest degree term of this series is of degree $i_0(f^q)$ and its coefficient is

$$\delta_0(f^q) \Big/ \prod_{w_0' \in O} (-w_0'); \tag{2.6}$$

which is therefore in $\mathcal{O}_k$. We thus have

$$|w_0|^q = \prod_{w_0' \in O} |w_0'| \geq |\delta_0(f^q)|\,, \tag{2.7}$$

and therefore (2.1). Moreover, equality holds precisely when the coefficient (2.6) of the lowest degree term of (2.5) has norm equal to 1. Thus, in view of Fact I stated at the beginning of the proof, it follows that equality in (2.7), and hence in (2.1), holds precisely when the Weierstrass degree of (2.5) is equal to $i_0(f^q)$. On the other hand, the cardinality of O is equal to q, and therefore the Weierstrass degree of (2.5) is equal to $\mathrm{wideg}(f^q(\zeta) - \zeta) - q - 1$. Combining these facts we conclude that equality in (2.1) holds if and only if we have (2.2). Finally, using the cardinality of O together with Facts I and II above, when this last equality holds, the set O is the set of all zeros of $(f^q(\zeta) - \zeta)/\zeta$ in $\mathfrak{m}_k$, so O is the only cycle of minimal period q of f. This completes the proof of part 1.

2. To prove (2.3), let $n \geq 1$ be an integer such that $i_{n-1}(f^q) < +\infty$, and ζ_0 in $\mathfrak{m}_k$ a periodic point of f of minimal period qp^n. By Lemma 2.5 with $g = f^{qp^{n-1}}$ and $m = p$, the power series $f^{qp^{n-1}}(\zeta) - \zeta$ divides $f^{qp^n}(\zeta) - \zeta$ in $\mathcal{O}_k[[\zeta]]$. Note that every point in the forward orbit O of ζ_0 in $\mathfrak{m}_k$ under f is a zero of the power series

$$h(\zeta) := \frac{f^{qp^n}(\zeta) - \zeta}{f^{qp^{n-1}}(\zeta) - \zeta},$$

and that the lowest degree term of this power series is of degree $i_n(f^q) - i_{n-1}(f^q)$ and its coefficient is equal to

$$\delta(h) := \frac{\delta_n(f^q)}{\delta_{n-1}(f^q)}.$$

On the other hand, O consists of qp^n points, and, since f maps $\mathfrak{m}_k$ to itself isometrically, all the points in O have the same norm. Applying Lemma 2.6 inductively with ξ replaced by each element of O, it follows that $\prod_{\zeta_0' \in O}(\zeta - \zeta_0')$ divides $h(\zeta)$ in $\mathcal{O}_k[[\zeta]]$. In particular, the power series $h(\zeta) / \prod_{\zeta_0' \in O}(\zeta - \zeta_0')$ is in $\mathcal{O}_k[[\zeta]]$, so the coefficient of its lowest degree term,

$$\left(\frac{\delta_n(f^q)}{\delta_{n-1}(f^q)} \right) / \prod_{\zeta_0' \in O} (-\zeta_0'), \tag{2.8}$$

is in $\mathcal{O}_k$. We thus have

$$|\zeta_0|^{qp^n} = \prod_{\zeta_0' \in O} |\zeta_0'| \geq \left| \frac{\delta_n(f^q)}{\delta_{n-1}(f^q)} \right|, \tag{2.9}$$

and therefore (2.3). Note that equality holds if and only if the lowest degree coefficient (2.8) of the power series $h(\zeta) / \prod_{\zeta_0' \in O}(\zeta - \zeta_0')$ has norm equal to 1. In view of Fact I stated at the beginning of the proof, we conclude that equality in (2.9), and hence in (2.3), holds if and only if

$$\operatorname{wideg} \left(h(\zeta) / \prod_{\zeta_0' \in O} (\zeta - \zeta_0') \right) = i_n(f^q) - i_{n-1}(f^q).$$

On the other hand, the cardinality of O is equal to qp^n, and therefore we have

$$\operatorname{wideg} \left(h(\zeta) / \prod_{\zeta_0' \in O} (\zeta - \zeta_0') \right) = \operatorname{wideg} \left(\frac{f^{qp^n}(\zeta) - \zeta}{f^{qp^{n-1}}(\zeta) - \zeta} \right) - qp^n.$$

Combining these facts, we conclude that equality holds in (2.3) if and only (2.4). Finally, using the cardinality of O together with Facts I and II, when this last equality holds O is the set of all zeros of $\frac{f^{qp^n}(\zeta) - \zeta}{f^{qp^{n-1}}(\zeta) - \zeta}$ in $\mathfrak{m}_k$, so O is the only cycle of minimal period qp^n of f. This completes the proof of part 2, and of the lemma. □

3. A reduction

In this section we prove Theorems A, B, and D assuming the following result, which is proved in §4. Note that for an odd integer q, each of the numbers $\frac{q-1}{2}$, $\frac{q+1}{2}$, and $\frac{q^2-1}{2}$ is an integer, and therefore defines an element on each field of characteristic 2.

Main Lemma. *Let p be a prime number, k a field of characteristic p, and $q \geq 1$ an integer that is not divisible by p. Given γ in k such that $\gamma^q = 1$, let $g(\zeta)$ be a power series in $k[[\zeta]]$ of the form*

$$g(\zeta) = \gamma\zeta \left(1 + \sum_{j=1}^{+\infty} a_j \zeta^{jq}\right). \tag{3.1}$$

Then we have

$$g^q(\zeta) \equiv \zeta \left(1 + q a_1 \zeta^q + q\left(\left(\frac{q^2-1}{2}\right) a_1^2 + a_2\right)\zeta^{2q}\right) \quad \bmod \left\langle \zeta^{3q+1} \right\rangle. \tag{3.2}$$

Moreover, if for a given integer $n \geq 1$ we put

$$\chi_{q,n} := \begin{cases} q a_1^{p^n - \frac{p^n-1}{p-1}} \left(\frac{q+1}{2} a_1^2 - a_2\right)^{\frac{p^n-1}{p-1}} & \text{if } p \text{ is odd;} \\ a_1 \left(\frac{q+1}{2} a_1^2 - a_2\right) & \text{if } p = 2 \text{ and } n = 1; \\ a_1 \left(\frac{q-1}{2} a_1^2 - a_2\right)^{2^{n-1}-1} \left(\frac{q+1}{2} a_1^2 - a_2\right)^{2^{n-1}} & \text{if } p = 2 \text{ and } n \geq 2, \end{cases}$$

and

$$\xi_{q,n} := \begin{cases} -q a_1^{p^n - \frac{p^n-1}{p-1} - 1} \left(\frac{q+1}{2} a_1^2 - a_2\right)^{\frac{p^n-1}{p-1}+1} & \text{if } p \text{ is odd;} \\ a_2^{2^{n-1}} \left(a_1^2 - a_2\right)^{2^{n-1}} & \text{if } p = 2, \end{cases}$$

then we have

$$g^{qp^n}(\zeta) \equiv \zeta \left(1 + \chi_{q,n} \zeta^{q\frac{p^{n+1}-1}{p-1}} + \xi_{q,n} \zeta^{q\frac{p^{n+1}-1}{p-1}+q}\right) \quad \bmod \left\langle \zeta^{q\frac{p^{n+1}-1}{p-1}+2q+1} \right\rangle. \tag{3.3}$$

The proof of the Main Lemma is given in §4. We now proceed to state some corollaries of this result that are used in the proofs of Theorems A, B and D, which are given in §3.1.

Corollary 3.1. *Let p be a prime number and k a field of characteristic p. Moreover, let γ be a root of unity in k, denote by q its order, and let $g(\zeta)$ be a power series in $k[[\zeta]]$ of the form* (3.1)*. If p is odd (resp. $p = 2$), then g is minimally ramified if and only if*

$$a_1 \neq 0 \text{ and } a_2 \neq \frac{q+1}{2} a_1^2 \quad \left(\text{resp. } a_1 \neq 0, a_2 \neq 0, \text{ and } a_2 \neq a_1^2\right).$$

Proof. When p is odd the corollary is a direct consequence of (3.2) and (3.3) in the Main Lemma. In the case $p = 2$ the integer q is odd, so we have $q = 1$ in k, and therefore by (3.2) we have $g^q(\zeta) \equiv \zeta(1 + a_1\zeta^q) \mod \langle \zeta^{2q+1} \rangle$. Moreover, in k we have either

$$\frac{q-1}{2} = 0 \text{ and } \frac{q+1}{2} = 1, \text{ or } \frac{q-1}{2} = 1 \text{ and } \frac{q+1}{2} = 0,$$

so either $\chi_{q,1} = a_1(a_1^2 - a_2)$ or $\chi_{q,1} = -a_1a_2$, and for each integer $n \geq 2$ we have either

$$\chi_{q,n} = -a_1 a_2^{2^{n-1}-1}(a_1^2 - a_2)^{2^{n-1}} \text{ or } \chi_{q,n} = a_1 a_2^{2^{n-1}}(a_1^2 - a_2)^{2^{n-1}-1}.$$

In view of (3.3), we conclude that g is minimally ramified if and only if $a_1 \neq 0$, $a_2 \neq 0$, and $a_2 \neq a_1^2$. This completes the proof of the corollary. □

Corollary 3.2. *Let p be a prime number and $(k, |\cdot|)$ an ultrametric field of characteristic p. Moreover, let γ be a root of unity in k, denote by q its order, and let $g(\zeta)$ be a power series in $\mathcal{O}_k[[\zeta]]$ of the form (3.1). Then for every integer $n \geq 1$ and every periodic point ζ_0 in $\mathfrak{m}_k$ of g of minimal period qp^n, we have*

$$|\zeta_0| \geq \begin{cases} |a_1|^{\frac{1}{q} - \frac{2}{qp}} \cdot \left| \frac{q+1}{2} a_1^2 - a_2 \right|^{\frac{1}{qp}} & \text{if } p \text{ is odd;} \\ \left| \frac{q+1}{2} a_1^2 - a_2 \right|^{\frac{1}{2q}} & \text{if } p = 2 \text{ and } n = 1; \\ \left| a_2 \left(a_1^2 - a_2 \right) \right|^{\frac{1}{4q}} & \text{if } p = 2 \text{ and } n \geq 2. \end{cases} \tag{3.4}$$

Moreover, if w_0 is a periodic point of g in $\mathfrak{m}_k \setminus \{0\}$ of minimal period q, then $|w_0| \geq |a_1|^{\frac{1}{q}}$. If in addition $a_1 = 0$, then we also have the bound $|w_0| \geq |a_2|^{\frac{1}{q}}$.

Proof. We use several times the fact that by definition p does not divide q and so $|q| = 1$.

We first consider the case $n = 0$. If $a_1 \neq 0$, then by (3.2) in the Main Lemma we have $\delta_0(g^q) = qa_1$. Together with (2.1) in Lemma 2.4, this implies $|w_0| \geq |a_1|^{\frac{1}{q}}$. Suppose $a_1 = 0$. Then we have $|w_0| \geq |a_1|^{\frac{1}{q}}$ trivially. If $a_2 = 0$, then the inequality $|w_0| \geq |a_2|^{\frac{1}{q}}$ also holds trivially. If $a_2 \neq 0$, then by (3.2) in the Main Lemma we have $\delta_0(g^q) = qa_2$. Then by (2.1) in Lemma 2.4 we obtain the non-trivial bound $|w_0| \geq |a_2|^{\frac{1}{q}}$.

We now consider the case where $n \geq 1$ and $\chi_{q,n} \neq 0$. By the Main Lemma we have $\delta_n(g^q) = \chi_{q,n}$. If in addition $n \geq 2$, then our assumption $\chi_{q,n} \neq 0$ implies $\chi_{q,n-1} \neq 0$, and by the Main Lemma we have $\delta_{n-1}(g^q) = \chi_{q,n-1}$. Combined with (2.3) in Lemma 2.4, this implies

$$|\zeta_0| \geq \left| \frac{\chi_{q,n}}{\chi_{q,n-1}} \right|^{\frac{1}{qp^n}} = \begin{cases} |a_1|^{\frac{1}{q} - \frac{2}{qp}} \cdot \left| \frac{q+1}{2} a_1^2 - a_2 \right|^{\frac{1}{qp}} & \text{if } p \text{ is odd;} \\ \left| a_2 \left(a_1^2 - a_2 \right) \right|^{\frac{1}{4q}} & \text{if } p = 2. \end{cases}$$

Suppose $n = 1$. Our assumption $\chi_{q,1} \neq 0$ implies $a_1 \neq 0$, and by (3.2) in the Main Lemma we have $\delta_0(g^q) = qa_1$. Then by (2.3) in Lemma 2.4, we have

$$|\zeta_0| \geq \left|\frac{\chi_{q,1}}{qa_1}\right|^{\frac{1}{qp}} = \begin{cases} |a_1|^{\frac{1}{q}-\frac{2}{qp}} \cdot \left|\frac{q+1}{2}a_1^2 - a_2\right|^{\frac{1}{qp}} & \text{if } p \text{ is odd;} \\ \left|\frac{q+1}{2}a_1^2 - a_2\right|^{\frac{1}{2q}} & \text{if } p = 2. \end{cases}$$

It remains to consider the case where $n \geq 1$ and $\chi_{q,n} = 0$. If p is odd, then $\chi_{q,n} = 0$ implies $a_1 = 0$ or $\frac{q+1}{2}a_1^2 - a_2 = 0$. In both cases the inequality (3.4) holds trivially. Suppose $p = 2$ and $n = 1$. Then our assumption $\chi_{q,1} = 0$ implies $a_1 = 0$ or $\frac{q+1}{2}a_1^2 - a_2 = 0$. In the latter case the inequality (3.4) holds trivially, so we assume $a_1 = 0$ and $\frac{q+1}{2}a_1^2 - a_2 \neq 0$, and therefore $a_2 \neq 0$. Then by 3.2 and (3.3) in the Main Lemma we respectively have

$$\delta_0(g^q) = qa_2 \text{ and } \delta_1(g^q) = \xi_{q,1} = -a_2^2.$$

So, by (2.3) in Lemma 2.4 we have $|\zeta_0| \geq |a_2|^{\frac{1}{2q}}$, which is (3.4) in this particular case. It remains to consider the case where $p = 2$ and $n \geq 2$. Note that our assumption $\chi_{q,n} = 0$ implies that $\chi_{q,n-1} = 0$. If either $a_1 = 0$ or $a_2 = a_1^2$, then the inequality (3.4) holds trivially, so we assume $a_1 \neq 0$ and $a_2 \neq a_1^2$. Then $\xi_{q,n} \neq 0$ and $\xi_{q,n-1} \neq 0$. Since $\chi_{q,n} = \chi_{q,n-1} = 0$, by the Main Lemma we have

$$\delta_n(g^q) = \xi_{q,n} \text{ and } \delta_{n-1}(g^q) = \xi_{q,n-1}.$$

Together with (2.3) in Lemma 2.4, this implies

$$|\zeta_0| \geq \left|\frac{\xi_{q,n}}{\xi_{q,n-1}}\right|^{\frac{1}{2^n q}} = \left|a_2\left(a_1^2 - a_2\right)\right|^{\frac{1}{4q}}.$$

This completes the proof of the corollary. □

3.1. **Proof of Theorems A, B, and D assuming the Main Lemma.** The proofs are given after the following lemma, which is an enhanced version of [LRL16, Proposition 4.1].

Lemma 3.3. *Let p be a prime number, let k a field of characteristic p, and denote by F the prime field of k. Fix a root of unity γ in k different from 1, and denote by $q \geq 2$ its order. Then for every integer $\ell \geq 1$ there are polynomials*

$$\alpha_\ell(x_1, \ldots, x_\ell) \text{ and } \beta_\ell(x_1, \ldots, x_{\ell q})$$

with coefficients in $F(\gamma)$, such that the following property holds. For every power series $f(\zeta)$ in $k[[\zeta]]$ of the form

$$f(\zeta) = \gamma\zeta\left(1 + \sum_{i=1}^{+\infty} c_i\zeta^i\right),$$

the power series

$$h(\zeta) := \zeta \left(1 + \sum_{\ell=1}^{+\infty} \alpha_\ell(c_1, \ldots, c_\ell) \zeta^\ell \right)$$

in $k[[\zeta]]$ *is such that*

$$h \circ f \circ h^{-1}(\zeta) = \gamma\zeta \left(1 + \sum_{j=1}^{+\infty} \beta_j(c_1, \ldots, c_{jq}) \zeta^{jq} \right).$$

Proof. Put $F_\infty := F(\gamma)[x_1, x_2, \ldots]$ and for each integer $m \geq 1$ put $F_m := F(\gamma)[x_1, \ldots, x_m]$. Moreover, consider the power series $\widehat{f}(\zeta)$ in $F_\infty[[\zeta]]$ defined by

$$\widehat{f}(\zeta) := \gamma\zeta \left(1 + \sum_{i=1}^{+\infty} x_i \zeta^i \right).$$

Let $s_0(\zeta)$ and $h_0(\zeta)$ be the polynomials in $F(\gamma)[\zeta]$ defined by

$$s_0(\zeta) := 1 \text{ and } h_0(\zeta) := \zeta.$$

We define inductively for every integer $\ell \geq 1$ polynomials $s_\ell(\zeta)$ and $h_\ell(\zeta)$ in $F_\ell[\zeta]$ of degrees at most $\ell + 1$ and $\left[\frac{\ell}{q}\right]$, respectively, such that

$$h_\ell(\zeta) \equiv h_{\ell-1}(\zeta) \mod \left\langle \zeta^{\ell+1} \right\rangle \tag{3.5}$$

and

$$s_\ell(\zeta) \equiv s_{\ell-1}(\zeta) \mod \left\langle \zeta^{\left[\frac{\ell-1}{q}\right]} \right\rangle, \tag{3.6}$$

and such that the power series $\widehat{f}_\ell(\zeta) := h_\ell \circ \widehat{f} \circ h_\ell^{-1}(\zeta)$ in $F_\infty[[\zeta]]$ satisfies

$$\widehat{f}_\ell(\zeta) \equiv \gamma\zeta s_\ell(\zeta^q) \mod \left\langle \zeta^{\ell+2} \right\rangle. \tag{3.7}$$

Note that

$$\widehat{f}_0(\zeta) := h_0 \circ \widehat{f} \circ h_0^{-1}(\zeta) = \widehat{f}(\zeta) \equiv \gamma\zeta \mod \left\langle \zeta^2 \right\rangle,$$

so (3.7) is satisfied when $\ell = 0$. Let $\ell \geq 1$ be an integer for which $s_{\ell-1}(\zeta)$ and $h_{\ell-1}(\zeta)$ are already defined and satisfy (3.7) with ℓ replaced by $\ell - 1$. Then there is $A(x_1, \ldots, x_\ell)$ in F_ℓ such that

$$\widehat{f}_{\ell-1}(\zeta) \equiv \gamma\zeta \left(s_{\ell-1}(\zeta^q) + A(x_1, \ldots, x_\ell)\zeta^\ell \right) \mod \left\langle \zeta^{\ell+2} \right\rangle.$$

In the case where ℓ is divisible by q, the congruence (3.7) is verified if we put

$$h_\ell(\zeta) := h_{\ell-1}(\zeta) \text{ and } s_\ell(\zeta) := s_{\ell-1}(\zeta) + A(x_1, \ldots, x_\ell)\zeta^{\frac{\ell}{q}}.$$

Suppose ℓ is not divisible by q. Then $\gamma^\ell - 1 \neq 0$, and

$$B(x_1, \ldots, x_\ell) := -(\gamma^\ell - 1)^{-1} A(x_1, \ldots, x_\ell)$$

defines a polynomial in F_ℓ. Consider the polynomial

$$h(\zeta) := \zeta \left(1 + B(x_1, \ldots, x_\ell)\zeta^\ell\right)$$

in $F_\ell[\zeta]$ and put

$$h_\ell(\zeta) := h \circ h_{\ell-1}(\zeta) \text{ and } s_\ell(\zeta) := s_{\ell-1}(\zeta).$$

Then we have

$$\widehat{f_\ell}(\zeta) = h_\ell \circ \widehat{f} \circ h_\ell^{-1}(\zeta) = h \circ \widehat{f}_{\ell-1} \circ h^{-1}(\zeta),$$

so there is $C(x_1, \ldots, x_\ell)$ in F_ℓ such that

$$\begin{aligned}\widehat{f_\ell}(\zeta) &\equiv \gamma\zeta \left(s_{\ell-1}(\zeta^q) + C(x_1, \ldots, x_\ell)\zeta^\ell\right) \mod \left\langle \zeta^{\ell+2} \right\rangle \\ &\equiv \gamma\zeta \left(s_\ell(\zeta^q) + C(x_1, \ldots, x_\ell)\zeta^\ell\right) \mod \left\langle \zeta^{\ell+2} \right\rangle.\end{aligned}$$

Thus, to complete the proof of the induction step it is enough to show that $C(x_1, \ldots, x_\ell) = 0$. To do this, note that by our definition of $B(x_1, \ldots, x_\ell)$ we have

$$\begin{aligned}h \circ \widehat{f}_{\ell-1}(\zeta) &= \widehat{f}_{\ell-1}(\zeta) \left(1 + B(x_1, \ldots, x_\ell)\widehat{f}_{\ell-1}(\zeta)^\ell\right) \\ &\equiv \gamma\zeta \left(s_{\ell-1}(\zeta^q) + A(x_1, \ldots, x_\ell)\zeta^\ell\right) \left(1 + B(x_1, \ldots, x_\ell)\gamma^\ell\zeta^\ell\right) \\ &\qquad \mod \left\langle \zeta^{\ell+2} \right\rangle \\ &\equiv \gamma\zeta \left(s_{\ell-1}(\zeta^q) + \left(A(x_1, \ldots, x_\ell) + B(x_1, \ldots, x_\ell)\gamma^\ell\right)\zeta^\ell\right) \\ &\qquad \mod \left\langle \zeta^{\ell+2} \right\rangle \\ &\equiv \gamma\zeta \left(s_{\ell-1}(\zeta^q) + B(x_1, \ldots, x_\ell)\zeta^\ell\right) \mod \left\langle \zeta^{\ell+2} \right\rangle.\end{aligned}$$

On the other hand

$$\begin{aligned}\widehat{f_\ell} \circ h(\zeta) &\equiv \gamma h(\zeta) \left(s_{\ell-1}(h(\zeta)^q) + C(x_1, \ldots, x_\ell)h(\zeta)^\ell\right) \mod \left\langle \zeta^{\ell+2} \right\rangle \\ &\equiv \gamma\zeta \left(1 + B(x_1, \ldots, x_\ell)\zeta^\ell\right) \left(s_{\ell-1}\left(\zeta^q\right) + C(x_1, \ldots, x_\ell)\zeta^\ell\right) \\ &\qquad \mod \left\langle \zeta^{\ell+2} \right\rangle \\ &\equiv \gamma\zeta \left(s_{\ell-1}\left(\zeta^q\right) + (B(x_1, \ldots, x_\ell) + C(x_1, \ldots, x_\ell))\zeta^\ell\right) \\ &\qquad \mod \left\langle \zeta^{\ell+2} \right\rangle.\end{aligned}$$

Comparing coefficients we conclude that $B(x_1, \ldots, x_\ell) = 0$. This completes the proof of the induction step and of (3.7).

For each integer $\ell \geq 1$ let $\alpha_\ell(x_1, \ldots, x_\ell)$ be the coefficient of $\zeta^{\ell+1}$ in $h_\ell(\zeta)$ and let $\beta_\ell(x_1, \ldots, x_{q\ell})$ be the coefficient of ζ^ℓ in $s_{q\ell}(\zeta)$. Then the power series

$$\widehat{h}(\zeta) := \zeta \left(1 + \sum_{\ell=1}^{+\infty} \alpha_\ell(x_1, \ldots, x_\ell)\zeta^\ell \right)$$

in $F_\infty[[\zeta]]$ is invertible, and by (3.5), (3.6), and (3.7) we have

$$\widehat{h} \circ \widehat{f} \circ \widehat{h}^{-1}(\zeta) = \gamma\zeta \left(1 + \sum_{j=1}^{+\infty} \beta_j(x_1, x_1, \ldots, x_{jq})\zeta^{jq} \right).$$

The proposition is obtained by specializing, for each integer $i \geq 1$, the variable x_i to c_i. □

Proof of Theorem A. Put

$$M_1(x_1, x_2) := \begin{cases} x_1 \left(x_1^2 - x_2 \right) & \text{if } p \text{ is odd;} \\ x_1 x_2 \left(x_1^2 - x_2 \right) & \text{if } p = 2, \end{cases}$$

and for $q \geq 2$, let $\beta_1(x_1, \ldots, x_q)$ and $\beta_2(x_1, \ldots, x_{2q})$ be the polynomials given by Lemma 3.3, and put

$$M_q(x_1, \ldots, x_{2q}) := \beta_1(x_1, \ldots, x_q) \left(\frac{q+1}{2} \beta_1(x_1, \ldots, x_q)^2 - \beta_2(x_1, \ldots, x_{2q}) \right),$$

if p is odd, and

$$\begin{aligned} &M_q(x_1, \ldots, x_{2q}) \\ &\quad := \beta_1(x_1, \ldots, x_q)\beta_2(x_1, \ldots, x_{2q}) \left(\beta_1(x_1, \ldots, x_q)^2 - \beta_2(x_1, \ldots, x_{2q}) \right), \end{aligned}$$

if $p = 2$.

By Corollary 3.1, in all the cases we have that a power series $f(\zeta)$ in $k[[\zeta]]$ of the form (1.2) is minimally ramified if and only if $M_q(c_1, \ldots, c_{2q}) \neq 0$. So, it only remains to prove that $M_q(x_1, \ldots, x_{2q}) \not\equiv 0$. When $q = 1$ this follows from the definition. To prove that $M_q(x_1, \ldots, x_{2q})$ is nonzero when $q \geq 2$, note that by Corollary 3.1 at least 1 of the following polynomials in $F(\gamma)[\zeta]$ is minimally ramified:

$$\gamma\zeta \left(1 + \zeta^q \right), \gamma\zeta \left(1 + \zeta^q + \gamma\zeta^{2q} \right).$$

Thus, either

$$M_q(\underbrace{0, \ldots, 0}_{q-1}, 1, \underbrace{0, \ldots, 0}_{q}) \text{ or } M_q(\underbrace{0, \ldots, 0}_{q-1}, 1, \underbrace{0, \ldots, 0}_{q-1}, \gamma)$$

is nonzero. This completes the proof of the theorem. □

Proof of Theorem B. Suppose $\gamma = 1$, so that $q = 1$, and let a_1 and a_2 be such that

$$f(\zeta) \equiv \zeta \left(1 + a_1\zeta + a_2\zeta^2 \right) \mod \left\langle \zeta^4 \right\rangle.$$

Since $i_0(f) = 1$, we have $a_1 \neq 0$ and $\delta_0(f) = a_1$, so by definition

$$\text{résit}(f) = 1 - \frac{a_2}{a_1^2}.$$

So the desired assertion is given by Corollary 3.2.

Suppose $\gamma \neq 1$, so that $q \geq 2$. By Lemma 3.3 there is a power series $h(\zeta)$ in $\mathcal{O}_k[[\zeta]]$ of the form

$$h(\zeta) = \zeta \left(1 + \sum_{\ell=1}^{+\infty} \alpha_\ell \zeta^\ell \right),$$

such that $g(\zeta) := h \circ f \circ h^{-1}(\zeta)$ is of the form (3.1). In particular, $h(\zeta_0)$ is a periodic point of g in $\mathfrak{m}_k$ of minimal period qp^n. Furthermore,

$$|h(\zeta_0) - \zeta_0| = |\zeta_0| \cdot \left| \sum_{\ell=1}^{+\infty} \alpha_\ell \zeta_0^\ell \right| \leq |\zeta_0|^2 < |\zeta_0|,$$

so $|h(\zeta_0)| = |\zeta_0|$. On the other hand, by Lemma 2.2, (3.2) in the Main Lemma, the fact that $f'(0) = g'(0)$, and our hypothesis $i_0(f^q) = q$, we have

$$i_0(f^q) = i_0(g^q) = q \text{ and } \delta_0(f^q) = \delta_0(g^q) = qa_1. \tag{3.8}$$

So, $a_1 \neq 0$ and by definition

$$\text{résit}(f) = \frac{q+1}{2} - \frac{a_2}{a_1^2}. \tag{3.9}$$

Then the desired estimate is a direct consequence of Corollary 3.2 applied to g, using $|h(\zeta_0)| = |\zeta_0|$ and that q is not divisible so $|q| = 1$. □

Proof of Theorem D. If $\gamma = 1$, and therefore $q = 1$, then the desired assertion is given by Corollary 3.1 with $g = f$.

Suppose $\gamma \neq 1$, so that $q \geq 2$. By Lemma 3.3 there is a power series $h(\zeta)$ in $k[[\zeta]]$ satisfying $h(\zeta) \equiv \zeta \mod \langle \zeta^2 \rangle$, such that $g(\zeta) := h \circ f \circ h^{-1}(\zeta)$ is of the form (3.1). Suppose f is minimally ramified. Then $i_0(f^q) = q$ and by Lemma 2.2 the power series g is minimally ramified. Moreover, by Corollary 3.1 we have $a_1 \neq 0$, so by definition we have (3.9). Then Corollary 3.1 implies that résit$(f) \neq 0$, and when $p = 2$ that résit$(f) \neq 1$. This completes the proof of the direct implication when $q \geq 2$. To prove the reverse implication, suppose $i_0(f^q) = q$, résit$(f) \neq 0$, and when $p = 2$ that résit$(f) \neq 1$. By Lemma 2.2 and (3.2) in the Main Lemma, we have (3.8) and $a_1 \neq 0$. So, by definition we have (3.9). Thus our assumptions on résit(f) and Corollary 3.1 imply that g is minimally ramified. By Lemma 2.2 the power series f is also minimally ramified. This completes the proof of the reverse implication in the case $q \geq 2$, and of the theorem. □

4. Generic parabolic points

The purpose of this section is to prove the Main Lemma stated in §3. The main ingredient is the following lemma, which is the case where $q = 1$ and $n \geq 1$. Note that the Main Lemma is trivial in the case where $q = 1$ and $n = 0$. The proof of the Main Lemma is at the end of this section.

Lemma 4.1 (The case $q = 1$ and $n \geq 1$)**.** *Let p be a prime number, k an ultrametric field of characteristic p, and*

$$f(\zeta) = \zeta + a\zeta^2 + b\zeta^3 + \cdots$$

a power series in $k[[\zeta]]$. Given an integer $n \geq 1$, put

$$\chi_n := \begin{cases} a^{p^n - \frac{p^n-1}{p-1}} \left(a^2 - b\right)^{\frac{p^n-1}{p-1}} & \text{if } p \text{ is odd;} \\ a\left(a^2 - b\right) & \text{if } p = 2 \text{ and } n = 1; \\ ab^{2^{n-1}-1}\left(a^2 - b\right)^{2^{n-1}} & \text{if } p = 2 \text{ and } n \geq 2, \end{cases}$$

and

$$\xi_n = \begin{cases} -a^{p^n - \frac{p^n-1}{p-1} - 1} \left(a^2 - b\right)^{\frac{p^n-1}{p-1}+1} & \text{if } p \text{ is odd;} \\ b^{2^{n-1}} \left(a^2 - b\right)^{2^{n-1}} & \text{if } p = 2. \end{cases}$$

Then we have

$$f^{p^n}(\zeta) \equiv \zeta \left(1 + \chi_n \zeta^{\frac{p^{n+1}-1}{p-1}} + \xi_n \zeta^{\frac{p^{n+1}-1}{p-1}+1}\right) \mod \left\langle \zeta^{\frac{p^{n+1}-1}{p-1}+3} \right\rangle. \tag{4.1}$$

Proof. The proof is divided into Cases 1.1, 1.2, 1.3 and 2.

Case 1.1. $p = 3$ and $n = 1$. For each integer $m \geq 1$ define the power series $\Delta_m(\zeta)$ in $k[[\zeta]]$ inductively by $\Delta_1(\zeta) := f(\zeta) - \zeta$, and for $m \geq 2$ by

$$\Delta_m(\zeta) := \Delta_{m-1}(f(\zeta)) - \Delta_{m-1}(\zeta).$$

Note that $\Delta_3(\zeta) = f^3(\zeta) - \zeta$. By definition $\Delta_1(\zeta)$ satisfies

$$\Delta_1(\zeta) \equiv a\zeta^2 + b\zeta^3 + c\zeta^4 \mod \left\langle \zeta^5 \right\rangle.$$

Using $p = 3$, we have

$$\Delta_2(\zeta) \equiv a\zeta^2 \left[\left(1 + a\zeta + b\zeta^2 + c\zeta^3\right)^2 - 1\right] + c\zeta^4 \left[(1 + a\zeta)^4 - 1\right] \mod \left\langle \zeta^6 \right\rangle.$$

Note that

$$\begin{aligned} \left(1 + a\zeta + b\zeta^2 + c\zeta^3\right)^2 - 1 &\equiv 2a\zeta + 2b\zeta^2 + 2c\zeta^3 + a^2\zeta^2 + 2ab\zeta^3 \mod \left\langle \zeta^4 \right\rangle \\ &\equiv -a\zeta + \left(a^2 - b\right)\zeta^2 - (ab + c)\zeta^3 \mod \left\langle \zeta^4 \right\rangle. \end{aligned}$$

Consequently, using $p = 3$ we thus have

$$\begin{aligned} \Delta_2(\zeta) &\equiv -a^2\zeta^3 + a\left(a^2 - b\right)\zeta^4 - \left(a^2b + ac\right)\zeta^5 + ac\zeta^5 \mod \left\langle \zeta^6 \right\rangle \\ &\equiv -a^2\zeta^3 + a\left(a^2 - b\right)\zeta^4 - a^2b\zeta^5 \mod \left\langle \zeta^6 \right\rangle, \end{aligned}$$

and

$$\begin{aligned} \Delta_3(\zeta) \equiv & -a^2\zeta^3 \left[\left(1 + a\zeta + b\zeta^2\right)^3 - 1\right] + a\left(a^2 - b\right)\zeta^4 \left[\left(1 + a\zeta + b\zeta^2\right)^4 - 1\right] \\ & - a^2b\zeta^5 \left[(1 + a\zeta)^5 - 1\right] \mod \left\langle \zeta^7 \right\rangle \\ \equiv & -a^5\zeta^6 + a^2\left(a^2 - b\right)\zeta^5 + ab\left(a^2 - b\right)\zeta^6 + a^3b\zeta^6 \mod \left\langle \zeta^7 \right\rangle \\ \equiv & \, a^2\left(a^2 - b\right)\zeta^5 - a\left(a^2 - b\right)^2\zeta^6 \mod \left\langle \zeta^7 \right\rangle. \end{aligned}$$

This completes the proof in the case where $p = 3$ and $n = 1$.

Case 1.2. $p \geq 5$ and $n = 1$. For each integer $m \geq 1$ define the power series $\Delta_m(\zeta)$ in $k[[\zeta]]$ inductively by $\Delta_1(\zeta) := f(\zeta) - \zeta$, and for $m \geq 2$ by

$$\Delta_m(\zeta) := \Delta_{m-1}(f(\zeta)) - \Delta_{m-1}(\zeta).$$

Note that $\Delta_p(\zeta) = f^p(\zeta) - \zeta$.

We first prove

$$\Delta_{p-3}(\zeta) \equiv -\frac{1}{2}a^{p-3}\zeta^{p-2} - \frac{3}{2}a^{p-2}\zeta^{p-1} \mod \langle \zeta^p \rangle . \tag{4.2}$$

To prove this, for integers $m \geq 1$ define α_m and β_m in k inductively by

$$\alpha_1 := 0, \quad \alpha_{m+1} := (m+2)\alpha_m + (m+1)!\frac{m}{2}, \tag{4.3}$$

and

$$\beta_1 := 1, \quad \beta_{m+1} := (m+2)\beta_m + (m+1)!. \tag{4.4}$$

We prove by induction that for $m \geq 1$ we have

$$\Delta_m(\zeta) \equiv m!a^m\zeta^{m+1} + \left(\alpha_m a^{m+1} + \beta_m a^{m-1} b\right)\zeta^{m+2} \mod \left\langle \zeta^{m+3} \right\rangle . \tag{4.5}$$

When $m = 1$ this is true by definition. Let $m \geq 1$ be such that (4.5) holds. Then

$$\begin{aligned}\Delta_{m+1}(\zeta) \equiv\ & m!a^m\zeta^{m+1}\left[\left(1 + a\zeta + b\zeta^2\right)^{m+1} - 1\right] \\ & + \left(\alpha_m a^{m+1} + \beta_m a^{m-1}b\right)\zeta^{m+2}\left[(1 + a\zeta)^{m+2} - 1\right] \\ & \mod \left\langle \zeta^{m+4} \right\rangle .\end{aligned}$$

Note that

$$\begin{aligned}\left(1 + a\zeta + b\zeta^2\right)^{m+1} - 1 \equiv (m+1)a\zeta + \left((m+1)b + \frac{(m+1)m}{2}a^2\right)\zeta^2 \\ \mod \left\langle \zeta^3 \right\rangle .\end{aligned}$$

Consequently,

$$\begin{aligned}\Delta_{m+1}(\zeta) \equiv\ & (m+1)!a^{m+1}\zeta^{m+2} + \left((m+1)!a^m b + (m+1)!\frac{m}{2}a^{m+2}\right)\zeta^{m+3} \\ & + \left((m+2)\alpha_m a^{m+2} + (m+2)\beta_m a^m b\right)\zeta^{m+3} \mod \left\langle \zeta^{m+4} \right\rangle .\end{aligned}$$

This completes the proof of the induction step and proves (4.5). To prove (4.2), first note that by (4.3) and using $\alpha_1 = 0$, we have for m in $\{2, \ldots, p-3\}$

$$\begin{aligned}
\frac{\alpha_m}{(m+1)!} &= \frac{\alpha_{m-1}}{m!} + \frac{1}{2} \cdot \frac{m-1}{m+1} \\
&= \frac{\alpha_{m-1}}{m!} + \frac{1}{2} - \frac{1}{m+1} \\
&= \frac{\alpha_1}{2!} + \frac{m-1}{2} - \left(\frac{1}{3} + \cdots + \frac{1}{m+1} \right) \\
&= \frac{m-1}{2} - \left(\frac{1}{3} + \cdots + \frac{1}{m+1} \right) \\
&= \frac{m+2}{2} - \left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{m+1} \right).
\end{aligned}$$

Consequently, for $m = p-3$, using $(p-2)! = 1$ we obtain $\alpha_{p-3} = -\frac{3}{2}$. So, to complete the proof of (4.2) it is enough to show that $\beta_{p-3} = 0$. To do this, note that using $\beta_1 = 1$ we have for every m in $\{2, \ldots, p-3\}$

$$\begin{aligned}
\frac{\beta_m}{(m+1)!} &= \frac{\beta_{m-1}}{m!} + \frac{1}{m+1} \\
&= \frac{\beta_1}{2!} + \frac{1}{3} + \cdots + \frac{1}{m+1} \\
&= \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{m+1}.
\end{aligned}$$

Hence, for $m = p-3$ we obtain $\beta_{p-3} = 0$, as required. This completes the proof of (4.2).

To complete the proof of (4.1) for $p \geq 5$ and $n = 1$, define A, B, and C in k by

$$\Delta_{p-3}(\zeta) = A\zeta^{p-2} + B\zeta^{p-1} + C\zeta^{p} + \cdots .$$

Note that by (4.2) we have

$$A = -\frac{1}{2}a^{p-3}, \text{ and } B = -\frac{3}{2}a^{p-2} = 3Aa. \tag{4.6}$$

By (4.2) and by definition of Δ_{p-2}, we have

$$\begin{aligned}
\Delta_{p-2}(\zeta) \equiv{} & A\zeta^{p-2} \left[\left(1 + a\zeta + b\zeta^2 + c\zeta^3\right)^{p-2} - 1 \right] \\
&+ 3Aa\zeta^{p-1} \left[\left(1 + a\zeta + b\zeta^2\right)^{p-1} - 1 \right] \\
&+ C\zeta^{p} \left[(1 + a\zeta)^{p} - 1 \right] \mod \left\langle \zeta^{p+2} \right\rangle .
\end{aligned}$$

Note that

$$\left(1 + a\zeta + b\zeta^2 + c\zeta^3\right)^{p-2} - 1 \equiv -2a\zeta + \left(3a^2 - 2b\right)\zeta^2 + \left(-4a^3 + 6ab - 2c\right)\zeta^3 \mod \left\langle \zeta^4 \right\rangle ,$$

and

$$\left(1 + a\zeta + b\zeta^2\right)^{p-1} - 1 \equiv -a\zeta + \left(a^2 - b\right)\zeta^2 \mod \left\langle \zeta^3 \right\rangle .$$

Since by assumption $2p \geq p+2$, we thus have

$$\begin{aligned}\Delta_{p-2}(\zeta) &\equiv -2aA\zeta^{p-1} + A\left(3a^2-2b\right)\zeta^p + A\left(-4a^3+6ab-2c\right)\zeta^{p+1} \\ &\quad - 3Aa^2\zeta^p + 3Aa\left(a^2-b\right)\zeta^{p+1} \mod \left\langle \zeta^{p+2}\right\rangle \\ &\equiv -2aA\zeta^{p-1} - 2Ab\zeta^p - A\left(a^3-3ab+2c\right)\zeta^{p+1} \mod \left\langle \zeta^{p+2}\right\rangle.\end{aligned}$$

Then we have

$$\begin{aligned}\Delta_{p-1}(\zeta) &\equiv -2Aa\zeta^{p-1}\left[\left(1+a\zeta+b\zeta^2+c\zeta^3\right)^{p-1}-1\right] \\ &\quad - 2Ab\zeta^p\left[\left(1+a\zeta+b\zeta^2\right)^p-1\right] \\ &\quad - A\left(a^3-3ab+2c\right)\zeta^{p+1}\left[(1+a\zeta)^{p+1}-1\right] \mod \left\langle \zeta^{p+3}\right\rangle.\end{aligned}$$

Note that

$$\left(1+a\zeta+b\zeta^2+c\zeta^3\right)^{p-1}-1 \equiv -a\zeta + \left(a^2-b\right)\zeta^2 + \left(-a^3+2ab-c\right)\zeta^3 \mod \left\langle \zeta^4\right\rangle.$$

Consequently, since by assumption $2p \geq p+3$, we thus have

$$\begin{aligned}\Delta_{p-1}(\zeta) &\equiv 2Aa^2\zeta^p - 2Aa\left(a^2-b\right)\zeta^{p+1} + 2Aa\left(a^3-2ab+c\right)\zeta^{p+2} \\ &\quad - Aa\left(a^3-3ab+2c\right)\zeta^{p+2} \mod \left\langle \zeta^{p+3}\right\rangle \\ &\equiv 2Aa^2\zeta^p - 2Aa\left(a^2-b\right)\zeta^{p+1} \\ &\quad + Aa^2\left(a^2-b\right)\zeta^{p+2} \mod \left\langle \zeta^{p+3}\right\rangle.\end{aligned}$$

It follows that, using $2p \geq p+4$, we have

$$\begin{aligned}\Delta_p(\zeta) &\equiv 2Aa^2\zeta^p\left[\left(1+a\zeta+b\zeta^2+c\zeta^3\right)^p-1\right] \\ &\quad - 2Aa\left(a^2-b\right)\zeta^{p+1}\left[\left(1+a\zeta+b\zeta^2\right)^{p+1}-1\right] \\ &\quad + Aa^2\left(a^2-b\right)\zeta^{p+2}\left[(1+a\zeta)^{p+2}-1\right] \mod \left\langle \zeta^{p+4}\right\rangle \\ &\equiv -2Aa^2\left(a^2-b\right)\zeta^{p+2} - 2Aab\left(a^2-b\right)\zeta^{p+3} \\ &\quad + 2Aa^3\left(a^2-b\right)\zeta^{p+3} \mod \left\langle \zeta^{p+4}\right\rangle \\ &\equiv -2Aa^2\left(a^2-b\right)\zeta^{p+2} + 2Aa\left(a^2-b\right)^2\zeta^{p+3} \mod \left\langle \zeta^{p+4}\right\rangle.\end{aligned}$$

Using $\Delta_p(\zeta) = f^p(\zeta)-\zeta$, $A = -a^{p-3}/2$, and the definitions of χ_1 and ξ_1, we obtain (4.1) in the case where $p \geq 5$ and $n = 1$.

Case 1.3. $p \geq 3$ and $n \geq 2$. We proceed by induction. Since (4.1) for $n=1$ was shown in Cases 1.1 and 1.2, we can assume that (4.1) holds for some integer $n \geq 1$. Put

$$g := f^{p^n}, \ d := \frac{p^{n+1}-1}{p-1}, \ \alpha := \chi_n, \ \text{and } \beta := \xi_n,$$

so there is γ in k such that

$$g(\zeta) \equiv \zeta + \alpha\zeta^{d+1} + \beta\zeta^{d+2} + \gamma\zeta^{d+3} \mod \left\langle \zeta^{d+4}\right\rangle.$$

Note that

$$d \geq 4,\ d \equiv 1 \mod p,\ \chi_{n+1} = -\alpha^{p-1}\beta,\ \text{and } \xi_{n+1} = -\alpha^{p-2}\beta^2. \tag{4.7}$$

For each integer $m \geq 1$ define the power series $\widehat{\Delta}_m(\zeta)$ in $k[[\zeta]]$ inductively by $\widehat{\Delta}_1(\zeta) := g(\zeta) - \zeta$, and for $m \geq 2$ by

$$\widehat{\Delta}_m(\zeta) := \widehat{\Delta}_{m-1}(g(\zeta)) - \widehat{\Delta}_{m-1}(\zeta).$$

Note that $\widehat{\Delta}_p(\zeta) = g^p(\zeta) - \zeta = f^{p^{n+1}}(\zeta) - \zeta$.

We first prove

$$\widehat{\Delta}_{p-2}(\zeta) \equiv \alpha^{p-2}\zeta^{(p-2)d+1} + \alpha^{p-3}\beta\zeta^{(p-2)d+2} + \alpha^{p-3}\gamma\zeta^{(p-2)d+3} \mod \left\langle \zeta^{(p-2)d+4} \right\rangle. \tag{4.8}$$

We then proceed to calculate $\widehat{\Delta}_{p-1}(\zeta)$ and $\widehat{\Delta}_p(\zeta)$ respectively. Note that (4.8) is true by definition when $p = 3$. To prove (4.8) for $p \geq 5$, we first prove

$$\widehat{\Delta}_{p-3}(\zeta) \equiv -\frac{1}{2}\alpha^{p-3}\zeta^{(p-3)d+1} \mod \left\langle \zeta^{(p-3)d+3} \right\rangle. \tag{4.9}$$

To prove this, for integers $m \geq 1$ we define C_m in k inductively by

$$C_1 := 1, \quad C_{m+1} := \prod_{j=1}^{m}(jd+1) + (md+2)C_m.$$

We prove by induction that for $m \geq 1$ we have

$$\widehat{\Delta}_m(\zeta) \equiv \left(\prod_{j=0}^{m-1}(jd+1)\right)\alpha^m\zeta^{md+1} + C_m\alpha^{m-1}\beta\zeta^{md+2} \mod \left\langle \zeta^{md+3} \right\rangle. \tag{4.10}$$

This follows by induction since it holds trivially for $m = 1$ and for $m \geq 1$ for which this holds we have

$$\begin{aligned}
\widehat{\Delta}_{m+1}(\zeta) \equiv & \left(\prod_{j=1}^{m-1}(jd+1)\right)\alpha^m\zeta^{md+1}\left[\left(1 + \alpha\zeta^d + \beta\zeta^{d+1}\right)^{md+1} - 1\right] \\
& + C_m\alpha^{m-1}\beta\zeta^{md+2}\left[\left(1 + \alpha\zeta^d\right)^{md+2} - 1\right] \mod \left\langle \zeta^{(m+1)d+3} \right\rangle \\
\equiv & \left(\prod_{j=1}^{m}(jd+1)\right)\alpha^{m+1}\zeta^{(m+1)d+1} \\
& + \alpha^m\beta\zeta^{(m+1)d+2}\left(\prod_{j=1}^{m}(jm+1) + (md+2)C_m\right) \\
& \mod \left\langle \zeta^{(m+1)d+3} \right\rangle.
\end{aligned}$$

We then prove that $C_{p-3} = 0$. Using that $d \equiv 1 \mod p$, for $m \geq 2$ we have that $\{C_m\}_{m\geq 1}$ satisfies the recursive relation

$$C_{m+1} = (m+1)! + (m+2)C_m,$$

with initial condition $C_1 = 1$. Hence $\{C_m\}_{m\geq 1}$ satisfies (4.4) and thus $C_{p-3} = 0$ as shown in Case 1.2. Moreover, using that for $m = p-3$ we have $(p-3)! = -1/2$ in k, from (4.10) we thus obtain (4.9) as asserted.

The congruence (4.9) implies that for some A in k the series $\widehat{\Delta}_{p-3}(\zeta)$ satisfies

$$\widehat{\Delta}_{p-3}(\zeta) \equiv -\frac{1}{2}\alpha^{p-3}\zeta^{(p-3)d+1} + A\zeta^{(p-3)d+3} \mod \left\langle \zeta^{(p-3)d+4} \right\rangle.$$

Using that $d \geq 4$ and that p divides $(p-3)d+3$, we thus have

$$\begin{aligned}\widehat{\Delta}_{p-2}(\zeta) \equiv & -\frac{1}{2}\alpha^{p-3}\zeta^{(p-3)d+1}\left[\left(1+\alpha\zeta^d+\beta\zeta^{d+1}+\gamma\zeta^{d+2}\right)^{(p-3)d+1} - 1\right] \\ & + A\zeta^{(p-3)d+3}\left[\left(1+\alpha\zeta^d\right)^{(p-3)d+3} - 1\right] \mod \left\langle \zeta^{(p-2)d+4} \right\rangle \\ \equiv & \ \alpha^{p-2}\zeta^{(p-2)d+1} + \alpha^{p-3}\beta\zeta^{(p-2)d+2} \\ & + \alpha^{p-3}\gamma\zeta^{(p-2)d+3} \mod \left\langle \zeta^{(p-2)d+4} \right\rangle.\end{aligned}$$

This completes the proof of (4.8).

Using that (4.8) holds for all $p \geq 3$, that $d \geq 4$, and p divides $(p-2)d+2$, we obtain

$$\begin{aligned}\widehat{\Delta}_{p-1}(\zeta) \equiv & \ \alpha^{p-2}\zeta^{(p-2)d+1}\left[\left(1+\alpha\zeta^d+\beta\zeta^{d+1}+\gamma\zeta^{d+2}\right)^{(p-2)d+1} - 1\right] \\ & + \alpha^{p-3}\beta\zeta^{(p-2)d+2}\left[\left(1+\alpha\zeta^d+\beta\zeta^{d+1}\right)^{(p-2)d+2} - 1\right] \\ & + \alpha^{p-3}\gamma\zeta^{(p-2)d+3}\left[\left(1+\alpha\zeta^d\right)^{(p-2)d+3} - 1\right] \mod \left\langle \zeta^{(p-1)d+4} \right\rangle \\ \equiv & -\alpha^{p-1}\zeta^{(p-1)d+1} - \alpha^{p-2}\beta\zeta^{(p-1)d+2} \\ & - \alpha^{p-2}\gamma\zeta^{(p-1)d+3} + \alpha^{p-2}\gamma\zeta^{(p-1)d+3} \mod \left\langle \zeta^{(p-1)d+4} \right\rangle \\ \equiv & -\alpha^{p-1}\zeta^{(p-1)d+1} - \alpha^{p-2}\beta\zeta^{(p-1)d+2} \mod \left\langle \zeta^{(p-1)d+4} \right\rangle.\end{aligned}$$

Using (4.7), we thus have

$$\begin{aligned}
\widehat{\Delta}_p(\zeta) &\equiv -\alpha^{p-1}\zeta^{(p-1)d+1}\left[\left(1+\alpha\zeta^d+\beta\zeta^{d+1}+\gamma\zeta^{d+2}\right)^{(p-1)d+1}-1\right]\\
&\quad -\alpha^{p-2}\beta\zeta^{(p-1)d+2}\left[\left(1+\alpha\zeta^d+\beta\zeta^{d+1}\right)^{(p-1)d+2}-1\right]\\
&\qquad \mod \left\langle \zeta^{pd+4}\right\rangle\\
&\equiv -\alpha^{p-1}\beta\zeta^{pd+2}-\alpha^{p-2}\beta^2\zeta^{pd+3} \mod \left\langle\zeta^{pd+4}\right\rangle.\\
&\equiv \chi_{n+1}\zeta^{pd+2}+\xi_{n+1}\zeta^{pd+3} \mod \left\langle\zeta^{pd+4}\right\rangle.
\end{aligned}$$

Using $\Delta_p(\zeta) = f^{p^{n+1}}(\zeta) - \zeta$ and the definition of d, this completes the proof of (4.1) for $p \geq 3$.

Case 2. $p = 2$. We proceed by induction. The case $n = 1$ follows from the fact that for $f(\zeta) = \zeta + a\zeta^2 + b\zeta^3 + c\zeta^4 + d\zeta^5 + \dots$ in $k[[\zeta]]$, using repeatedly that $p = 2$, we have

$$\begin{aligned}
f^2(\zeta) \equiv& \zeta\left(1+a\zeta+b\zeta^2+c\zeta^3+d\zeta^4\right)+a\zeta^2\left(1+a\zeta+b\zeta^2+c\zeta^3\right)^2\\
&+b\zeta^3\left(1+a\zeta+b\zeta^2\right)^3+c\zeta^4\left(1+a\zeta\right)^4+d\zeta^5 \mod \langle\zeta^6\rangle\\
\equiv& \left(\zeta+a\zeta^2+b\zeta^3+c\zeta^4+d\zeta^5\right)+a\zeta^2\left(1+a^2\zeta^2\right)\\
&+b\zeta^3\left(1+a\zeta+b\zeta^2\right)\left(1+a^2\zeta^2\right)+c\zeta^4+d\zeta^5 \mod \langle\zeta^6\rangle\\
\equiv& \zeta+a(a^2-b)\zeta^4+b(a^2-b)\zeta^5 \mod \langle\zeta^6\rangle.
\end{aligned}$$

Let $n \geq 1$ be an integer for which (4.1) holds, and note that

$$\chi_{n+1} = \chi_n \cdot \xi_n \text{ and } \xi_{n+1} = \xi_n^2. \tag{4.11}$$

Put

$$\widetilde{\Delta}_1(\zeta) := f^{2^n}(\zeta) - \zeta \text{ and } \widetilde{\Delta}_2(\zeta) := \widetilde{\Delta}_1\left(f^{2^n}(\zeta)\right) - \widetilde{\Delta}_1(\zeta),$$

and note that $\widetilde{\Delta}_2(\zeta) = f^{2^{n+1}}(\zeta) - \zeta$. By our induction hypothesis there is A in k such that

$$\widetilde{\Delta}_1(\zeta) \equiv \chi_n\zeta^{2^{n+1}} + \xi_n\zeta^{2^{n+1}+1} + A\zeta^{2^{n+1}+2} \mod \left\langle\zeta^{2^{n+1}+3}\right\rangle,$$

and therefore

$$\begin{aligned}
\widetilde{\Delta}_2(\zeta) \equiv& \chi_n\zeta^{2^{n+1}}\left[\left(1+\chi_n\zeta^{2^{n+1}-1}+\xi_n\zeta^{2^{n+1}}+A\zeta^{2^{n+1}+1}\right)^{2^{n+1}}-1\right]\\
&+\xi_n\zeta^{2^{n+1}+1}\left[\left(1+\chi_n\zeta^{2^{n+1}-1}+\xi_n\zeta^{2^{n+1}}\right)^{2^{n+1}+1}-1\right]\\
&\qquad\qquad \mod \left\langle\zeta^{2^{n+2}+2}\right\rangle.
\end{aligned}$$

Note that

$$\left(1+\chi_n\zeta^{2^{n+1}-1}+\xi_n\zeta^{2^{n+1}}+A\zeta^{2^{n+1}+1}\right)^{2^{n+1}}-1 \equiv 0 \mod \left\langle\zeta^{2^{n+1}+2}\right\rangle,$$

and

$$\left(1+\chi_n\zeta^{2^{n+1}-1}+\xi_n\zeta^{2^{n+1}}\right)^{2^{n+1}+1}-1$$
$$\equiv \chi_n\zeta^{2^{n+1}-1}+\xi_n\zeta^{2^{n+1}} \mod \left\langle \zeta^{2^{n+1}+1}\right\rangle.$$

We thus have by (4.11)

$$\begin{aligned} f^{2^{n+1}}(\zeta)-\zeta=\widetilde{\Delta}_2(\zeta) &\equiv \chi_n\xi_n\zeta^{2^{n+2}}+\xi_n^2\zeta^{2^{n+2}+1} \mod \left\langle \zeta^{2^{n+2}+2}\right\rangle \\ &\equiv \chi_{n+1}\zeta^{2^{n+2}}+\xi_{n+1}\zeta^{2^{n+2}+1} \mod \left\langle \zeta^{2^{n+2}+2}\right\rangle. \end{aligned}$$

This completes the proof of the induction step, and hence of the lemma in the case $p=2$.

The proof of Lemma 4.1 is thus complete. □

Lemma 4.2. *Let p be a prime number, k a field of characteristic p, and*

$$f(\zeta)=\zeta+a\zeta^2+b\zeta^3+\cdots$$

a power series in $k[[\zeta]]$. Then for every integer $\ell\geq 1$ we have

$$f^{\ell}(\zeta)\equiv \zeta+\ell a\zeta^2+(\ell(\ell-1)a^2+\ell b)\zeta^3 \mod \left\langle \zeta^4\right\rangle. \tag{4.12}$$

Proof. We proceed by induction. When $\ell=1$ the congruence (4.12) holds by definition of f. Let $\ell\geq 1$ be an integer for which (4.12) holds. Then

$$\begin{aligned} f^{\ell+1}(\zeta) &\equiv \zeta+\ell a\zeta^2+\left(\ell(\ell-1)a^2+\ell b\right)\zeta^3+a\left[\zeta+\ell a\zeta^2\right]^2+b\zeta^3 \mod \left\langle \zeta^4\right\rangle \\ &\equiv \zeta+(\ell+1)a\zeta^2+\left[(\ell(\ell-1)+2\ell)a^2+(\ell+1)b\right]\zeta^3 \mod \left\langle \zeta^4\right\rangle \\ &\equiv \zeta+(\ell+1)a\zeta^2+\left[(\ell+1)\ell a^2+(\ell+1)b\right]\zeta^3 \mod \left\langle \zeta^4\right\rangle. \end{aligned}$$

This completes the induction step and hence the proof of (4.12) as required. □

Proof of the Main Lemma. The case where $q=1$ and $n=0$ is trivial and the case where $q=1$ and $n\geq 1$ is given by Lemma 4.1. In what follows we assume $q\geq 2$. Put

$$\pi(\zeta):=\zeta^q \text{ and } \widehat{g}(\zeta):=\zeta\left(1+\sum_{j=1}^{+\infty}a_j\zeta^j\right)^q,$$

and note that $\pi\circ g=\widehat{g}\circ\pi$. Clearly

$$\widehat{g}(\zeta)\equiv \zeta+qa_1\zeta^2+\left(\frac{q(q-1)}{2}a_1^2+qa_2\right)\zeta^3 \mod \left\langle \zeta^4\right\rangle.$$

Using Lemma 4.2 with $\ell = q$, $a = qa_1$, and $b = \frac{q(q-1)}{2}a_1^2 + qa_2$, we obtain

$$\begin{aligned}
\widehat{g}^q(\zeta) &\equiv \zeta + q(qa_1)\zeta^2 \\
&\quad + \left[q(q-1)(qa_1)^2 + q\left(\frac{q(q-1)}{2}a_1^2 + qa_2\right)\right]\zeta^3 \mod \left\langle \zeta^4 \right\rangle \\
&\equiv \zeta + q^2 a_1 \zeta^2 \\
&\quad + q^2\left[\left(q(q-1) + \frac{q-1}{2}\right)a_1^2 + a_2\right]\zeta^3 \mod \left\langle \zeta^4 \right\rangle \\
&\equiv \zeta + q^2 a_1 \zeta^2 + q^2\left[\left(q^2 - \frac{q+1}{2}\right)a_1^2 + a_2\right]\zeta^3 \mod \left\langle \zeta^4 \right\rangle .
\end{aligned} \tag{4.13}$$

Let A_0, A_1, $\ldots$, A_q in k be such that

$$g^q(\zeta) \equiv \zeta\left(1 + A_0\zeta^q + \cdots + A_q\zeta^{2q}\right) \mod \left\langle \zeta^{2q+2} \right\rangle .$$

Then we have

$$\pi \circ g^q(\zeta) \equiv \zeta^q\left(1 + qA_0\zeta^q + \cdots + qA_{q-1}\zeta^{2q-1} + \left(\frac{q(q-1)}{2}A_0^2 + qA_q\right)\zeta^{2q}\right) \mod \left\langle \zeta^{3q+1} \right\rangle .$$

Together with the semi-conjugacy $\pi \circ g^q = \widehat{g}^q \circ \pi$ and with (4.13), this implies

$$A_0 = qa_1, A_1 = \cdots = A_{q-1} = 0, \text{ and } A_q = q\left[\left(\frac{q^2-1}{2}\right)a_1^2 + a_2\right].$$

This proves the desired assertion when $n = 0$.

Fix an integer $n \geq 1$. By the semi-conjugacy $\pi \circ g^q = \widehat{g}^q \circ \pi$, we have $\pi \circ g^{qp^n} = \widehat{g}^{qp^n} \circ \pi$. On the other hand, by (4.13), the definitions of $\chi_{q,n}$ and $\xi_{q,n}$, the fact that $q^p = q$ in k, and by Lemma 4.1 with

$$a = q^2 a_1 \text{ and } b = q^2\left(q^2 - \frac{q+1}{2}\right)a_1^2 + q^2 a_2,$$

we have, using

$$a^2 - b = q^2\left(\frac{q+1}{2}a_1^2 - a_2\right),$$

that

$$\widehat{g}^{qp^n}(\zeta) \equiv \zeta\left(1 + q\chi_{q,n}\zeta^{\frac{p^{n+1}-1}{p-1}} + q\xi_{q,n}\zeta^{\frac{p^{n+1}-1}{p-1}+1}\right) \mod \left\langle \zeta^{\frac{p^{n+1}-1}{p-1}+3} \right\rangle . \tag{4.14}$$

Together with $\pi \circ g^{qp^n} = \widehat{g}^{qp^n} \circ \pi$, this implies that there are constants B_0, $B_1, \ldots, B_q$ in k such that

$$g^{qp^n}(\zeta) \equiv \zeta \left(1 + B_0 \zeta^{q\frac{p^{n+1}-1}{p-1}} + \cdots + B_q \zeta^{q\frac{p^{n+1}-1}{p-1}+q}\right) \mod \left\langle \zeta^{q\frac{p^{n+1}-1}{p-1}+q+2} \right\rangle.$$

Consequently, we have

$$\pi \circ g^{qp^n}(\zeta) \equiv \zeta^q \left(1 + qB_0 \zeta^{q\frac{p^{n+1}-1}{p-1}} + \cdots + qB_q \zeta^{q\frac{p^{n+1}-1}{p-1}+q}\right) \mod \left\langle \zeta^{q\frac{p^{n+1}-1}{p-1}+q+2} \right\rangle.$$

Using $\pi \circ g^{qp^n} = \widehat{g}^{qp^n} \circ \pi$ and (4.14), it follows that

$$B_0 = \chi_{q,n}, B_1 = \cdots = B_{q-1} = 0, \text{ and } B_q = \xi_{q,n}.$$

This completes the proof of the Main Lemma. □

References

[Éca75] J. Écalle. Théorie itérative: introduction à la théorie des invariants holomorphes. *J. Math. Pures Appl. (9)*, 54:183–258, 1975.

[HY83] M. Herman and J.-C. Yoccoz. Generalizations of some theorems of small divisors to non-Archimedean fields. In *Geometric dynamics (Rio de Janeiro, 1981)*, volume 1007 of *Lecture Notes in Math.*, pages 408–447. Springer, Berlin, 1983.

[Kea92] Kevin Keating. Automorphisms and extensions of $k((t))$. *J. Number Theory*, 41(3):314–321, 1992.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[Lin04] Karl-Olof Lindahl. On Siegel's linearization theorem for fields of prime characteristic. *Nonlinearity*, 17(3):745–763, 2004.

[Lin10] Karl-Olof Lindahl. Divergence and convergence of conjugacies in non-Archimedean dynamics. In *Advances in p-adic and non-Archimedean analysis*, volume 508 of *Contemp. Math.*, pages 89–109. Amer. Math. Soc., Providence, RI, 2010.

[LMS02] François Laubie, Abbas Movahhedi, and Alain Salinier. Systèmes dynamiques non archimédiens et corps des normes. *Compositio Math.*, 132(1):57–98, 2002.

[LRL16] Karl-Olof Lindahl and Juan Rivera-Letelier. Optimal cycles in ultrametric dynamics and minimally ramified power series. *Compositio Math.*, 152:187–222, 2016.

[LS98] F. Laubie and M. Saïne. Ramification of some automorphisms of local fields. *J. Number Theory*, 72(2):174–182, 1998.

[Lub94] Jonathan Lubin. Non-Archimedean dynamical systems. *Compositio Math.*, 94(3):321–346, 1994.

[RL03] Juan Rivera-Letelier. Dynamique des fonctions rationnelles sur des corps locaux. *Astérisque*, (287):xv, 147–230, 2003. Geometric methods in dynamics. II.

[Sen69] Shankar Sen. On automorphisms of local fields. *Ann. of Math. (2)*, 90:33–46, 1969.

[Win04] Jean-Pierre Wintenberger. Automorphismes des corps locaux de caractéristique p. *J. Théor. Nombres Bordeaux*, 16(2):429–456, 2004.

[Yoc95] Jean-Christophe Yoccoz. Théorème de Siegel, nombres de Bruno et polynômes quadratiques. *Astérisque*, (231):3–88, 1995. Petits diviseurs en dimension 1.

Karl-Olof Lindahl, Department of Mathematics, Linnaeus University, 351 95, Växjö, Sweden
E-mail address: karl-olof.lindahl@lnu.se

Juan Rivera-Letelier, Facultad de Matemáticas, Pontificia Universidad Católica de Chile, Avenida Vicuña Mackenna 4860, Santiago, Chile
E-mail address: riveraletelier@mat.puc.cl
URL: http://rivera-letelier.org/